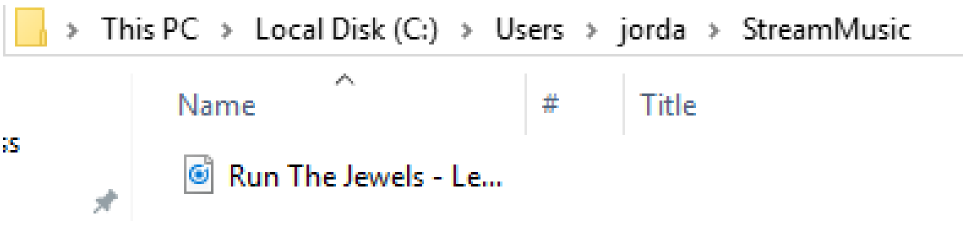
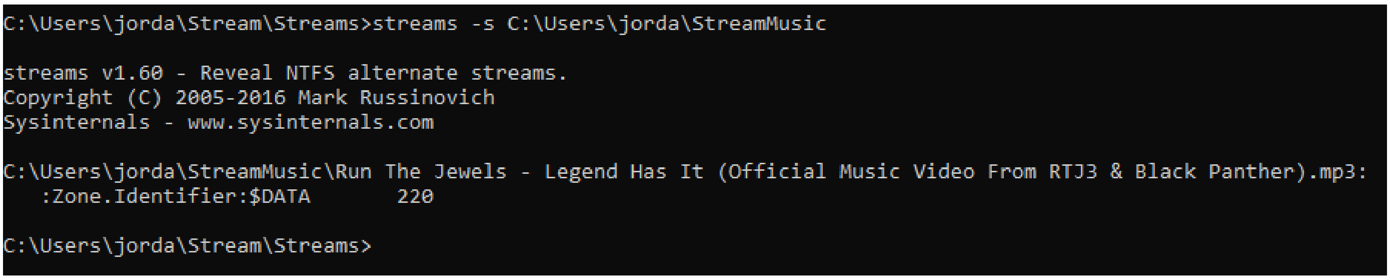
Week 10 Forensics lab

If we go to the sysInternals and download the stream utility v1.6 we are given a folder with two executable files and a text file. The next step is to extract the folder to its own location and open up the command window and go to that location. We now make another folder and in that we have a music file.



We then run the command “streams -s C://nameOfTheLocation”.This shows us our song, but it also hides files in a stream.



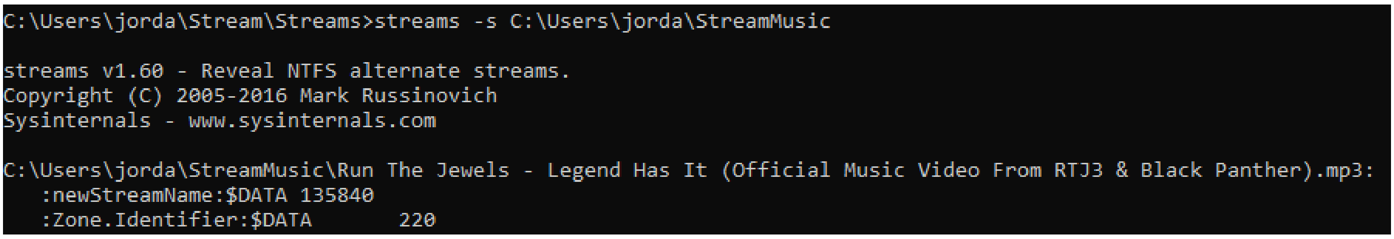
```
C:\Users\jorda\Stream\Streams>streams -s C:\Users\jorda\StreamMusic

streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\jorda\StreamMusic\Run The Jewels - Legend Has It (Official Music Video From RTJ3 & Black Panther).mp3:
   :Zone.Identifier:$DATA       220

C:\Users\jorda\Stream\Streams>
```

If we run the command TYPE "ExeLocation" > "NameOfSong.mp3" :newStreamName we will create a new stream. What this command will do is copy the stream and hide the file. If we run the streams -s file, we can see this. The picture below as there are now 2 streams.



```
C:\Users\jorda\Stream\Streams>streams -s C:\Users\jorda\StreamMusic

streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Users\jorda\StreamMusic\Run The Jewels - Legend Has It (Official Music Video From RTJ3 & Black Panther).mp3:
   :newStreamName:$DATA 135840
   :Zone.Identifier:$DATA       220
```